특 집

DigiPass : KoreaSat DBS의 Conditional Access System

趙 賢 淑, 林 春 植
韓國電子通信研究所

I. 서 론

최근 위성의 상업적 이용의 확대와 더불어 위성에 의한 직접위성방송(Direct Broadcasting Satellite)이 도입되고 있으며, 음성 및 영상 신호 전송도 디지탈화로 가는 추세이다. 종래의 지상방송 중심의 TV 방송은 위성방송이 디지탈 전송시스템으로 변화함에 따라 TV 신호를 디지탈 처리 및 전송을 가능케 하여, 신호 전송의 높은 비화도를 가질 수 있으며, 영상 화질의 향상을 꾀할 수 있다. 또한, 위성을 이용한 직접위성방식은 수신료를 납부한 가입자만이 방송을 수신할 수 있는 가입자개념으로 변환을 특징으로 한다. 기존의 방송서비스에 가입자개념의 추가는 방송국이 광고료 수입에만 의존하지 않고 시청자들로부터 징수한 수신료에 의해 방송국 운영이 가능케 되었으며, 종래의 지상방송에 비해 방송 내용의 질적인 측면에서 차별화된 특수 채널의 탄생을 가능케 하여 수신료를 시청시간 및 시청한 프로그램에 따라 차등 적용하는 등 다양한 서비스 제공 기능을 가능케 해주나, 위성방송은 누구나 시청할 수 있다는 전파상의 특성 때문에, 조건부 접근 제어(Conditional Access Control : 본 고에서는 제한 수신으로 명명) 기능의 역할에 대한 개념이 중요하게 대두 되었다.

그리하여, Pay-TV 시스템에서 제한수신기능을 이용하여 TV 방송에 가입자 개념을 추가하여 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하고, 전문 방송업자들에 의한 전문 방송 프로그램의 제작을 가능케 하여 다양한 기능의 서비스를 제공할 수 있게 되었다. 또한, 가입자 개념을 가지는 상업 방송의 높은 부가가치성에 대한 인식으로 몇몇 선진국에서는 제한 수신에 대한 연구가 상당히 진척되어 있으며, 상용 서비스의 제공은 물론, HDTV의 개발 및 신호 전송의 디지탈화에 발맞추어 디지탈 TV의 신호 스크램블링 기술 역시 상당한 수준에 이르고 있다. NewsData-Com사의 상용화 Conditional Access System인 VideoCrypt는 세계 최초로 미국의 디지탈 위성방송서비스를 하고 있는 DirecTV에 사용되고 있으

며, France Telecom VigioPass의 CAS 시스템인 Eurocrypt, GI의 DigiCipher 등을 들 수 있다. 이외에도 CATV, VOD, 멀티미디어 시대의 Interactive TV 서비스에 활용을 위한 CAS 시스템 개발이 유럽을 중심으로 활발히 진행되고 있다. 국내에서도 무궁화위성 발사와 발맞추어 디지탈방식에 의한 직접위성방송 서비스에서의 Pay-TV Service를 위한 제한수신시스템인 DigiPass 시스템 개발이 진행되고 있다.

본 고에서는 디지탈방송에서의 제한수신 기능 및 KoreaSat DBS의 제한수신시스템인 DigiPass (Digital all Pass : Audio/Vidio /Data) 시스템에 대해서 논하고자 한다.

II. CAS : Conditional Access System

제한수신시스템(CAS)이란 송신기에서 스크램블된 신호를 수신측의 수신 인가를 받은 가입자만이 디스크램블하여 프로그램을 시청할 수 있도록 하는 시스템으로, 이 시스템이 갖추어야 하는 기본적인 요건은 첫째로, 시청료를 지불한 정단한 가입자만이 프로그램을 시청할 수 있어야 하고, 둘째, 미가입자의 불법 도시청을 막을 수 있는 스크램블링의 강도가 높아야 될 뿐만 아니라, 디스클램블링에 필요한 키를 알아내는 것을 막을 수 있어야 한다.

1. CAS의 기능 요구사항

디지탈 TV 방송에서의 제한수신시스템의 기본 요구조건을 만족시키기 위해 다음의 두 가지 기능을 고려해야 한다.

첫째, 프로그램 및 데이타는 스크램블링되고 통신 링크상에서 보호되어야 하며, 둘째, 인증을 위한 가입자 신분 확인(Authentication)기능과 접근제어(Access Control) 기능이 있어야 한다.

위의 두 가지 기능은 결국 자원(프로그램 및 데이타)과 가입자 보호를 위한 것으로, 자원의 보호메카니즘으로는 스크램블링/디스크램블링이 있고, 가입자 보호메카니즘으로는 인가된 가입자들에게 해당 시청 권한을 주는 기술이다. 자격(Entitlement)은 프로그램 및 데이타의 스크램블링에 필요한 관련 키와 수신자의 시청 권리를 말하며 자격통제와 자격관리로 대별할 수 있다.

(1) 스크램블링/디스크램블링 기능(Scrambling/Descrambling Function)

스크램블링은 원래의 신호에 변형을 가하여 스크램블된 형태의 신호만으로는 수신권한이 없는 수신자는 시청할 수 없도록 하는 것으로 신호의 종류(영상,음성, 데이타) 및 신호의 형태(아날로그, 디지탈)에 따라 스크램블링의 방식이 달라진다. 디스크램블링은 스크램블된 프로그램을 원래의 신호대로 복원하는 과정을 말하며, 결국 제어 워드(control word, CW)라는 파라미터를 가진 수신기들에서만 디스크램블된 프로그램의 시청이 가능하다. 신호의 질을 손상시키지 않고 스크램블링/디스램블링 하는 과정은 아날로그 신호보다는 디지탈에서 더 간단하다. 스크램블링의 안전도는 결국 스크램블링을 위해서 생성되는 의사 난수열의 안전도에 의존하며, 디지탈 신호를 스크램블링하기 위해서 블럭 암호화 같은 방법이 사용될 수 있으나, 스크램블링의 가장 쉽고 빠른 방법은 PRBS (Pseudo Random Byte Sequences)생성기에 의해 생성된 PRBS에 exculsive-OR하는 방법이다. PRBS 생성기에 초기 데이타는 CW(Control Word)와 계수기(period counter)로 만들어지며, 이 CW는 스크램블러와 인가된 디스크램블러들에게만 알려진 secret parameter이다. CW는 불법 도시청을 위한 공격 대상에서 피하기 위해 충분히 길어야 하고, 자주 변경되어야 한다. 예를들어 34~45Mb/s TV codec에 대한 conditional access ssyetem은 64bits의 CW를 가지고 8.2초마다 갱신시킨다. 계수기(period counter)는 스크램블러와 디스크램블러의 PRBS 생성기에서의 동기화를 위한 변수이며, 이 계수기는 PRBS 생성기들을 재초기화하고, 그들은 긴 sequences를 출력을 조정하는 역할을 한다. 따라서, 이 계수기가 나타내는 주기 동안에는 자격 조건을 변경시키는 일련의 과정은 발생하지 않는다.

(2) 자격통제기능(Entitlement Control Function)

프로그램을 디스크램블하기 위해 필요로 한 권한과 관련 키들을 entitlements라 한다. 이 기능은 암호화된 control words와 프로그램을 access하기 위해서 필요로 한 요구 조건들을 분배, 즉 난수 발생의 초기치인 제어워드(Control Word : CW)를 암호화하고 그 제어 워드를 자격 통제 메시지(Entitlement Control Message : ECM)를 통해 전송한다. 수신기는 이 ECM을 받게 되면, 암호화된 CW와 제어 조건들을 스마트 카드라고 하는 security device로 보내게 되어, 스마트 카드는 먼저 합당한 데이타인지를 check한 후 CW를 복호화하여 디스크램블러로 보내게 되며, 가입자는 디스크램블된 프로그램을 시청할 수 있다. ECM은 보통 한 개의 패킷으로 구성되어 주기적으로 전송되며, 그 때마다 새로운 CW가 암호화되어 전송된다. CW를 주기적으로 바꾸는 이유는 스크램블링의 의사 난수의 규칙성을 찾을 수 없도록 하여 비화도를 높이려는 것이다. 자격 통제 메시지내에는 암호화된 CW외에 프로그램 정보와 access parameter도 함께 전송된다. 모든 수신기는 전송된 자격 통제 메시지를 수신할 수 있으며, 그 중 CW와 access parameter를 수신기와 접속된 스마트 카드로 전달하고, 스마트 카드에서는 프로그램 취득 조건 및 자격을 심사한 후 정당한 수신자로 판명되면, 스마트 카드내의 서비스 키를 이용하여 CW를 해독하고 디스크램블에 필요한 난수의 초기치를 발생한다. 자격 통제 메시지의 송/수신은 ECM의 주기 계수기(period counter)에 의해 방송될 프로그램과 동기화된다.

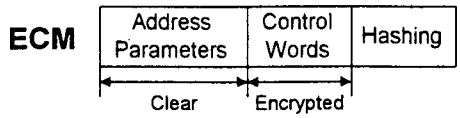
(3) 자격관리기능(Entitlement Management Function)

자격관리기능은 가입자들에게 자격(entitlements)을 전달하는 기능으로 이 데이타는 EMM (Entitlement Managements Messages)라는 메시지에 실어서 보낸다. EMM은 수신기의 보안장치인 스마트 카드내에 자격을 부여하거나 갱신하는 기능을 지원하며, 각 수신자의 주소에 의한 인식 기능을 이용하여 수신자의 서비스 키를 바꾸거나 통제하는 통제 취득기능의 지원도 가능하다. 자격 관리기능은 앞으로 시청할 프로그램의 수신자격에 대한 정보관리 기능이므로 batch 동작으로 실행된다. 따라서, 전송할 프로그램과 동기화되어 전달될 필요는 없으며, EMM을 형성하여 특수 채널을 통해 방송되거나 우편등의 매체로도 전달 가능하다.

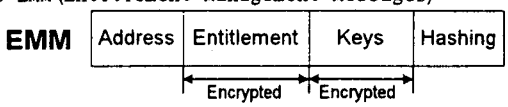
위의 자격 통제 기능과 자격 관리 기능의 지원을 수행하기 위해 비밀키와 암호화 알고리즘이 요구되며, 사용하며, 새로이 설계된 대부분의 제한 수신 시스템은 정보를 안전하게 저장하고 수행하기 위해 보통 스마트 카드를 사용하고 있다.

(4) 메시지 구조

o ECM (Entitlement Control Messages)

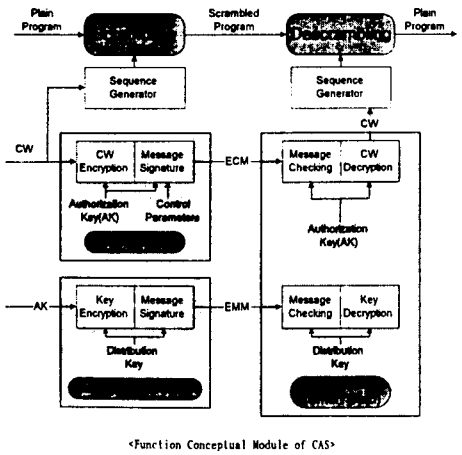


o EMM (Entitlement Management Messages)



〈그림 1〉

2. CAS의 기능 구성도



<Function Conceptual Module of CAS>

〈그림 2〉

III. 안전성 서비스 및 메카니즘(Security Servuces & Mechanisms)

1. Conditional Access를 위한 안정성 서비스 (Security Service)

수신료를 지불한 정당한 가입자에게 안전한 서비스를 제공하기 위한 사용자의 보안서비스에 대한 기능으로는 우선 안전성(security)을 들 수 있는데, 시스템의 안전성은 비인가된 사용자가 서비스를 시도할 때 마주치게 되는 어려움의 정도로서 여기에는 두 가지 양상이 있다. 즉 Access Control과는 상관없이 관련 신호를 디스크램블링하는 것으로 이것은 서비스가 나타내는 성질과 스크램블링에 의한 함수로 고려할 수 있고, 또 하나는 불법적인 방법으로 접근키를 얻는 것으로서, 사용되는 알고리즘의 안전성 문제와 키 관리방법상의 문제로 생각할 수 있다.

OSI Security Structure(ISO 7498-2)에서 제안한 안전성 서비스는 신분확인 서비스(Authentication Service), 엑세스 제어 서비스(Access Control Service), 비밀성서비스(Integrity Service), 데이타 무결성 서비스(Data Integrity Service) 및 부인 봉쇄(Non-repudiation) 등이 제시되어 있으며, DigiPass 시스템에서 제공하는 안전성 서비스는 가입자에게 안전한 서비스를 제공하기 위해서 가입자 인증서비스(Authentication Service), 비밀성 서비스(Integrity Service) 및 Access Control Service 등이다. 안전성서비스의 비밀성(Confidentiality)은 정보의 내용과 가입자의 정보가 보호되어야 하는 것이며, 통계 및 과금 처리를 위해 필요한 수신자 인증(Authentication) 기능도 제공되어야 한다.

2. 안정성 메카니즘(Security Mechanism)

제한 수신을 위한 안전성 메카니즘(security mechanism)으로는 스크램블링/디스크램블링, 의사 난수 발생, 암/복호화, 인증 프로토콜, 키 관리 등이 있다. 이러한 메카니즘을 안전하게 수행하기 위한 방법으로 보통 스마트 카드를 사용하고 있다. 스마트 카드는 암호키를 안전하게 저장할 수 있고 필요한 암호학적 기능을 수행하는 안전한 장비로서, 자신의 소유자의 암호키를 안전하게 유지하고 그리고 사용된 암호시스템을 구현한 하드웨어 메카니즘 및 소프트웨어 메카니즘을 포함하고 있으며, 이는 합법적인 개인에게만 부여된다.

3. 스마트 카드

Smart Card는 신용 카드와 같은 크기의 플라스틱으로 둘러 쌓인 메모리를 가진 micro-computer chip이라 하며, 메모리로의 모든 accesses는 microchip내에 있는 CPU에 의해서 control되고, 외부장치와의 인터페이스는 serial asynchronous eletrical bus를 통해서 수행된다. 스마트 카드의 dimensions, 기계적 특성 및 전기적 인터페이스는 ISO 7816에서 규정하고 있다.

스마트 카드의 microchip은 기본적으로 다른 micro-controller chip과 같은 구조로서 스마트 카드용 CPU는 8-bit 혹은 16-bit processor로서 ROM, RAM, 혹은 EEPROM에 access를 한다. 스마트 카드의 메모리는 외부장치와 직접 통신할 수 없고, 모든 access는 serial I/O link를 통해 CPU에 의해서만 가능하다. 기존의 microcomputer chip들과는 달리, 스마트 카드는 안전성 목적을 위해서 특별히 설계되었으며, 구조 역시 안전성을 위해서 최적화 되었다.

스마트 카드와 접속되는 수신기는 프로그램 시청 권한을 가진 데이타들을 스마트 카드 내에 저장하고, 스마트 카드는 real-time으로 복호화 알고리즘을 처리하는 active device이다. 카드를 decoder로부터 카드를 꺼내게 되면, decoder는 디스크램블링하기 위해서 필요로한 데이타를 더 이상 제공하지 않는다.

IV. 제한 수신 기능의 처리

1. 프로그램 제공자(Program Provider)

프로그램 제공자는 프로그램을 직접 제작하거나 다른 제공자들로부터 구하여 프로그램을 제공한다.

제한수신기능이 필요한 프로그램에 대해서 접근조건(access conditions)을 정의하여 ECM을 생성하여 계산하는 제어장비(control device)로 보내게 된다.

프로그램 제공자는 프로그램이 방송될 시간을 결정해야 하고, CW 변경에 대해서도 제어가 가능해야 한다. 여러 프로그램에 대해서 같은 접근조건(access condition)을 사용하는 것이 가능하다. 이 경우에 모든 프로그램은 같은 ECM을 공유하게 되며, 또 하나의 ECM이 여러 프로그램에 의해서도 공유가 가능한데, 이런 일련의 결정들은 모두 프로그램 제공자에 의해서 이루어진다. 또한, 프로그램 제공자는 스크램블된 프로그램 및 데이타에 대해서 스크램블링 모드와 관련 자격 통제 메시지를 정의해야 하며, 해당 모드와 자격 통제 메시지는 프로그램 제공자에 의해서 어느 때든지 변경이 가능하나, 이런 처리는 1초 이내에 이루어져 실제 시청자들은 이런 변화를 느낄 수 없어야 한다.

마찬가지로, 프로그램 제공자는 시청자에게 새로운 자격을 보내기 위해서 EMM을 사용하여 방송시청 권한에 관련된 정보들을 포함한다.

2. 방송국(Broadcaster)

스크램블링 기술을 적용하여, 정보의 전송을 책임지며, ECM에 대한 자원을 할당하며, 제어 장비로부터 받은 ECM을 다중화기(multiplexer)에 넣는다.

방송 다중화기(Broadcast multiplexer)는 여러 프로그램에 대해서 뿐만 아니라, 심지어 다른 여러 장소에서 사용되는 ECM을 반복하지 않고 여러 프로그램들은 하나의 ECM을 사용하여 전송할 수 있도록 한다. 또한, ECM에 대한 자원을 할당하며, 관리 장비(management device)로부터 받은 EMM을 다중화기에 넣는 기능도 가지고 있다.

그리고 프로그램 제공자가 결정한 스크램블링 모드에 따라 프로그램들을 스크램블링해야 하는데, 스크램블러와 디스크램블러의 동기를 빠르고 쉽게 하기 위해서 초기화 수정자의 빈번한 변경이 요구된다. 이런 일련의 운용을 위해서 방송국은 방송 다중화가 제공해야 하는 동기화 파라미터와 스크램블링 기법을 사용한다.

3. 수신기 디코더(User Decoder)

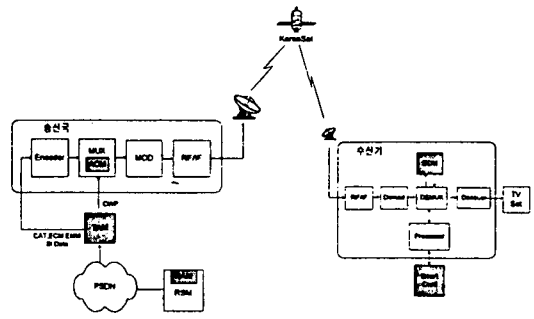
신호의 demodulation, 채널 디코딩, 역다중화 및 디스크램블링 기능을 수행하는 수신측의 디코더는 디스크램블링 운용을 쉽고 간단하게 하기 위해서, 단지 하나의 알고리즘만을 사용할 것을 권고하고 있다. 디코더는 가입자가 선정한 프로그램에 대한 ECM을 찾아서 수신자의 자격을 점검하고, CW를 계산하기 위해서 그 메시지를 수신측의 보안 모듈(User Security Module) 즉, 스마트 카드로 보낸다.

ECM은 제때에 CW를 얻기 위해서 전송 및 계산상의 지연을 고려하여 미리(적어도 150ms 이전) 수신자의 스마트 카드로 보내져야 하며, 이러한 문제의 해결을 위해서 실질적으로 두 개의 ECMs(current CW, next CW)을 사용한다.

V. DigiPass : KoreaSat DBS의 Conditional Access System

1. 구성

무궁화위성방송시스템에서의 Conditional Access 기능 실현을 위한 시스템인 DigiPass는 5기능 모듈(그림 참조) 즉, RAM(RSM Access Module), TAM(TS Access Module), ACM(Acce-ss Control Module), DDM(Digital Descrambler Module), SSC(Subscriber Smart Card)로 구성된다. RAM과 TAM은 가입자 관리시스템



〈그림 3〉 DigiPass 시스템 구성도

에, ACM은 송신국에, DDM과 SSC는 수신기에 각각 위치한다.

2. 기능 및 서비스

(1) 기능

RAM(RSM Access Manager)

RAM은 RSM의 다른 Manager(DBM, RRM)로부터 가입자 Entitlement 정보와 프로그램에 대한 정보를 받는다. 이 정보를 이용하여 RAM은 local DB에 필요한 정보를 update하고, EMM을 생성한다. EMM은 수신 자격을 갖춘 가입자에게만 수신을 허용하기 위해서 암호화 되어야 하며, 이 암호화에 필요한 키 관리 역시 RAM에서 수행한다.

생성한 EMM과 TAM에서 필요로하는 정보를 최대 6대의 TAM으로 전송하여야 한다. 이 정보의 내용은 ECM을 생성하기 위한 프로그램/채널 정보, program Service Information을 생성하기 위한 초기 데이타, ECM 암호화를 위한 키 정보 등이다.

TAM(Transmitter Access Manager)

TAM은 크게 나누어서 두 가지 역할을 한다. 첫째 RAM으로부터 전송되어 온 가입자관리 데이타(EMM, RCM, PAT, PMT, CAT, NIT, SDT, TDT, EIT)를 Transmitter의 DATA 입력 장치까지 전달한다. 둘째 Program을 Scrambling하기 위한 Control Word를 주기적으로 생성하고 이를 ACM에 전달하며, 권한을 가진 가입자들이 Descrambling하여 원래의 Program을 볼 수 있도록 하기 위한 Message인 ECM을 생성하여 Transmitter에 전송한다. 따라서 TAM은 RAM으로 부터의 하나의 입력과 ACM, Transmitter로의 두 개의 출력 통로를 가진다.

비 정기적인 전송 형태를 가지는 Messages(EMM, TDT, RCM)은 RAM에서 전송되어 온 형태를 그대로 Transmitter에 전달한다. 정기적인 전송형태를 가지는Messages(PAT, PMT, CAT, NIT, SDT, EIT) 등은 일단 TAM내에 저장한 다음, 전송 주기에 맞도록 반복적으로 Transmitter에 전달한다. TAM내에서 생성하는 Control Word는 주기적으로 만들어질 때마다 ACM에 전달하며, ECM은 Channel 전환시에도 빠르게 Descrambling이 가능하도록 Control Word 변경 주기내에 여러 차례 반복하여 Transmitter로 전송한다.

ACM(Access Control Manager)

ACM은 TAM에서 전송되어온 Control Word을 이용하여 각 Program을 권한이 없는 가입자가 알아볼 수 없는 형태로 변환한다. 이를 Scrambling이라 한다. ACM은 송신기의 MUX와 밀결합(tightly coupled) 형태로 되어 있으며 MPEG-II의 Transport Stream Packet 단위로 Scrambling 할 수 있다. 각 Program은 Video 혹은 Audio 만을 Scrambling할 수 있고, Video와 Audio 모두를 Scrambling 할 수도 있다.

DDM(Digital Descrambler Module)

이 모듈은 송신기로부터의 수신 제한을 위해 스크램블된 video/audio/data 신호를 스마트 카드로부터 받은 CW를 이용하여 원래의 신호로 복호화하는 기능을 담당한다.

SSC(Subscriber Smart Card)

수신기에는 스마트 카드에 대한 인터페이스를 가지고 있으며, 이 스마트 카드에는 가입자에 대한 정보뿐만 아니라 가입자의 Pay-TV 시청 이력과 수신 자격을 판단하기 위한 암호 키와 알고리즘을 저장하고 있다.

스마트 카드는 수신기로부터 암호화된 EMM과 ECM을 받아서 인증과정을 거친후 해당 가입자가 수신 자격을 갖고 있음을 확인하면 EMM내의 키를 복호화하고 이 키를 이용하여 ECM으로부터 CW를 추출한다. 이 CW는 DDM으로 전송되어 스크램블된 video/audio/data 신호의 디스크램블에 이용한다.

스마트 카드에 저장된 내용은 아래와 같다.

- 가입자 정보(subscriber id, PIN)
- Entiltements(channel id, expiry time,

keys)
- 수신 이력(channel id, start time, end time)
- 암호/인증 알고리즘

(2) 서비스

제한수신시스템이 갖추어야 하는 기본 요건들은 다음과 같다.
- 제어키 보호를 위한 적절한 암호화 알고리즘 선정 및 키 관리 방법 보장
- 서비스 이용기간, 프로그램 및 서비스 등급 및 서비스 요금과 같은 다양한 제어모드 지원
- 자격을 가진 가입자에게 해당 서비스의 수신권한을 부여하는 자격제어 및 관리 기능 지원

이러한 기본요건을 바탕으로, 무궁화위성방송에서는 DigiPass 시스템의 기능을 이용하여 다음과 같은 방송서비스를 제공한다.
- 주제별/프로그램 서비스 등급별 가입
- 다수의 프로그램 서비스 등급 및 주제에 대한 동시 가입
- Pre-Booked Pay-Per-View(PPV)
- Impulse Pay-Per-View
- 위성을 통한 시청자격 제어 및 관리
- 수신권리 부여기간의 제한
- PPV 수요촉진을 위한 Pay Free Time
- 스마트 카드를 이용한 가입자 보호관리 및 사용통계 데이타관리

VI. 결 론

제한수신에 대한 일반적인 기능은 위성을 이용한 디지탈 위성방송에서 뿐만 아니라 CATV (Cable TV), VOD 등 멀티미디어 서비스에서의 Pay-TV 서비스를 위해 다양한 기능을 제공에 적용할 수 있다. 최근 방송 추세는 채널마다 전문성을 지니며 다른 방송과 구별이 되는 전문 방송채널의 확대 및 방송 사업자의 수입을 광고료에 의존하지 않고 가입자의 시청료에 의존하여 방송 내용의 질적 차별화를 추구하고 있다.

또한, 데이타의 전송 방식에 있어서도 기존의 아날로그 방식에서 탈피해 디지탈화로 나아가고 있으며, HDTV 등 보다 나은 화질과 음질 등 고품질의 서비스 제공을 추구하고 있다. 이런 추세에 직접위성방송과 CATV 같은 방송 기술 및 제한수신 기능의 지원을 위한 기술은 필수적이며 잠재적으로 매우 높은 부가 가치를 지니고 있다. 아직까지 이와 관계된 기술은 미국, 유럽 등 기술 선진국들이 독점하고 있으며, 이에 대한 기술 개발에 주력하지 않는다면 기술 종속으로 인한 엄청난 피해를 입게 될 수도 있을 것이다. 국내에 독자적인 기술 개발로 이러한 앞선 기술들을 먼저 획득한다면 기술 선진국들에 대한 기술 종속을 피할 수 있을 뿐만 아니라 기술 수출까지도 꾀할 수 있을 것이다.

참 고 문 헌

[1] Information processing system-Open Systems Interconnection-Basic Reference Model-Part 2 : Security Architecture, ISO 7498-2.

[2] General characteristics of a conditional access broadcasting system-Report CCIR 1079-1.

저 자 소 개

趙 賢 淑

1957年 12月 28日
1980年 2月 전남대학교 수학 학사
1991年 8月 충북대학교 전산학 석사

1982年 3月～현재 한국전자통신연구소 선임연구원

주관심분야 : Cryptography, Communication Security

林 春 植

1952年 4月 3日
1975年 2月 한국항공대학 통신공학과(공학사)
1986年 2月 한국항공대학 대학원 석사과정(통신전공)
1992年 3月 일본 요코하마 국립대학 전자정보공학과박사과정 (전자정보) 수료

1978年 3月 군복무(공군 ROTC)
1980年 6月 국방과학연구소(연구원)
1995年 6月 현재 한국전자통신연구소 위성통신연구단 지상시스템부 부장 (책임연구원)

주관심 연구분야 : 정보이론(채널 코딩), 디지틀 이동통신, 대역확산통신, 위성통신망 및 신호처리 기술